doi.org/10.51891/rease.v11i6.19753

O DIREITO À PRIVACIDADE NA ERA DIGITAL; DESAFIOS E FUNDAMENTOS JURIDICOS DE FORMA OBJETIVA

Stheffany Pereira da Costa[1]
Janderson Gabriel Frota Januário[2]

RESUMO: O presente artigo analisa o direito à privacidade na era digital, destacando os principais desafios jurídicos decorrentes do avanço tecnológico e da crescente circulação de dados pessoais. O objetivo é compreender como os fundamentos legais, tanto no âmbito nacional quanto internacional, buscam proteger os direitos dos indivíduos frente às práticas de coleta, armazenamento e compartilhamento de informações. A metodologia utilizada é de caráter qualitativo, baseada em pesquisa bibliográfica e documental, abordando legislações como a Lei Geral de Proteção de Dados (LGPD) e princípios constitucionais. O estudo evidencia que, embora haja avanços normativos, persistem desafios significativos na efetivação da privacidade, especialmente diante de práticas empresariais e governamentais que, muitas vezes, desconsideram os limites éticos e legais na gestão de dados. Conclui-se que a consolidação de uma cultura de proteção à privacidade exige não apenas o fortalecimento dos instrumentos jurídicos, mas também a conscientização social e o desenvolvimento de mecanismos técnicos que garantam a segurança informacional dos cidadãos.

Palavras-chave: Privacidade digital. Proteção de dados. Fundamentos jurídicos. Segurança da informação. Sociedade da informação.

1 INTRODUÇÃO

O presente trabalho tem como objeto de pesquisa o direito à privacidade na era digital, com enfoque nos desafios enfrentados e nos fundamentos jurídicos que sustentam sua proteção no ordenamento jurídico brasileiro. A pesquisa delimita-se à análise das normas que regulam a proteção de dados pessoais, como a Constituição Federal de 1988, a Lei nº 12.965/2014 (Marco Civil da Internet) e a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD), além da Emenda Constitucional nº 115/2022, que elevou a proteção de dados ao patamar de direito fundamental.

A justificativa para o estudo reside na crescente coleta e uso de dados pessoais em ambientes digitais por empresas e plataformas tecnológicas, frequentemente sem o devido

[1]Discente no curso de direito.
[2]Orientador no curso de direito.

conhecimento ou consentimento dos usuários. Diante desse cenário, a proteção da privacidade torna-se um imperativo jurídico e social, essencial para preservar a dignidade, a autonomia e a liberdade dos indivíduos, fundamentos indispensáveis para uma sociedade democrática.

O problema de pesquisa que orienta este estudo é: como as legislações estão abordando o desafio de equilibrar a proteção dos dados pessoais com a necessidade de segurança e inovação tecnológica na era digital? A hipótese levantada é a de que, embora existam normas jurídicas consistentes, como a LGPD e os dispositivos constitucionais, ainda há obstáculos relevantes em sua aplicação prática, como a falta de conscientização da população, a dificuldade de fiscalização e a insuficiência das estruturas técnicas e institucionais para garantir a efetividade da proteção da privacidade.

O objetivo geral é analisar os desafios e fundamentos jurídicos do direito à privacidade na era digital. Os objetivos específicos são: 1) analisar a legislação vigente, especialmente a Constituição Federal e a LGPD; 2) investigar os desafios práticos enfrentados na implementação das normas de proteção de dados; e 3) explorar a responsabilidade das plataformas digitais na coleta e tratamento de dados pessoais.

O referencial teórico está baseado nas contribuições de autores como Solove (2008), que discute a privacidade como dimensão da dignidade e liberdade humanas; Schneier (2015), que destaca a importância da segurança da informação; e Gonçalves (2020), que analisa os avanços e os desafios da LGPD. Também são exploradas as obras de Zuboff (2019), que problematiza o "capitalismo de vigilância", e Nery Jr. (2020), que comenta os principais dispositivos da LGPD.

A metodologia adotada é qualitativa, descritiva e explicativa, com base em pesquisa bibliográfica e documental. Foram utilizados livros, artigos científicos, legislações nacionais e internacionais e decisões jurisprudenciais. A pesquisa tem natureza básica e busca ampliar o conhecimento teórico sobre o tema, sem pretensão imediata de aplicação prática.

A estrutura do trabalho está dividida em três seções principais: a primeira analisa a legislação vigente sobre privacidade e proteção de dados; a segunda aborda os desafios práticos enfrentados na aplicação dessas normas; e a terceira trata da responsabilidade das plataformas digitais. Por fim, são apresentadas as conclusões obtidas a partir da análise e sugestões para a efetivação do direito à privacidade no contexto digital contemporâneo.

2 ANALISAR A LEGISLAÇÃO VIGENTE: EXAMINAR AS PRINCIPAIS DISPOSIÇÕES DA CONSTITUIÇÃO FEDERAL E DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) QUE GARANTEM O DIREITO À PRIVACIDADE, IDENTIFICANDO SEUS PONTOS FORTES E FRACOS EM RELAÇÃO À PROTEÇÃO DOS DADOS PESSOAIS NA ERA DIGITAL

A evolução do direito à privacidade no Brasil está intimamente ligada ao desenvolvimento do Estado Democrático de Direito e à consolidação dos direitos fundamentais na Constituição Federal de 1988. Essa trajetória histórica reflete a crescente valorização da intimidade e do controle individual sobre as informações pessoais, em especial diante das transformações tecnológicas que intensificaram a coleta e o uso de dados.

O marco inicial mais relevante no ordenamento jurídico brasileiro é o artigo 5º, inciso X, da Constituição Federal, que consagra como invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas. Segundo Duarte (2019), essa norma constitucional representa um pilar de proteção à dignidade humana, ao reconhecer a privacidade como valor essencial à liberdade e à autonomia do indivíduo. No entanto, o autor também aponta que, embora a norma tenha grande relevância jurídica, sua efetiva aplicação enfrenta obstáculos práticos, especialmente diante de práticas invasivas que muitas vezes ocorrem de forma silenciosa e sem o conhecimento do titular dos dados.

Com o avanço da digitalização e a globalização da economia da informação, tornou-se evidente a necessidade de um arcabouço normativo mais específico. Nesse contexto, a promulgação da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados (LGPD), marcou uma mudança histórica na regulação do tratamento de dados pessoais no Brasil. Inspirada em modelos internacionais, como o Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia, a LGPD introduziu uma série de princípios e regras que conferem maior transparência e controle aos titulares de dados. Como destaca Nery Jr. (2020), a norma estabelece fundamentos claros — como a finalidade, a necessidade e o consentimento — e confere ao cidadão o direito de acessar, corrigir e revogar o uso de suas informações, fortalecendo a autonomia informacional no ambiente digital.

Contudo, o contexto histórico de implementação da LGPD revela desafios persistentes. Como aponta Câmara (2021), a eficácia da legislação é limitada pela fragilidade das estruturas de fiscalização, pela insuficiência de profissionais qualificados e pela resistência de parte do setor privado em adaptar suas práticas. Tais entraves refletem um descompasso entre os

avanços normativos e a realidade operacional do país, o que compromete o pleno alcance das garantias previstas.

A incorporação da proteção de dados pessoais no rol de direitos fundamentais da Constituição Federal , por meio da Emenda Constitucional nº 115/2022, representa outro marco histórico relevante. Essa alteração reafirma o compromisso do Estado brasileiro com a proteção da privacidade em um cenário global cada vez mais orientado por dados e algoritmos.

Adicionalmente, conforme alerta Mourão (2022), a historicidade da proteção à privacidade não pode ser dissociada das transformações tecnológicas contemporâneas. O surgimento de ferramentas como a inteligência artificial e a mineração de dados amplia significativamente os riscos à privacidade, exigindo uma interpretação dinâmica e evolutiva da legislação vigente. Nesse sentido, a construção histórica do direito à privacidade no Brasil é marcada por avanços legislativos importantes, mas também por desafios contínuos que demandam uma atuação integrada do poder público, do setor privado e da sociedade civil.

3 INVESTIGAR OS DESAFIOS PRÁTICOS: AVALIAR OS DESAFIOS ENFRENTADOS NA IMPLEMENTAÇÃO DAS NORMAS DE PRIVACIDADE E PROTEÇÃO DE DADOS, INCLUINDO A FALTA DE CONSCIENTIZAÇÃO DOS CIDADÃOS, AS DIFICULDADES DE FISCALIZAÇÃO E A NECESSIDADE DE ADAPTAÇÃO DAS EMPRESAS ÀS EXIGÊNCIAS LEGAIS

A implementação efetiva das normas de privacidade e proteção de dados no Brasil, especialmente após a entrada em vigor da Lei Geral de Proteção de Dados (LGPD), tem enfrentado diversos desafios práticos que comprometem o pleno exercício dos direitos assegurados aos titulares de dados. Tais dificuldades abrangem desde a conscientização da população até entraves estruturais nas empresas e nos órgãos fiscalizadores.

Um dos primeiros e mais relevantes obstáculos é a falta de conscientização da população em geral sobre seus direitos relacionados à proteção de dados. Conforme destaca Vilela (2020), mesmo após a promulgação da LGPD, grande parte da sociedade brasileira ainda desconhece os mecanismos legais disponíveis para exercer direitos como o acesso, a retificação ou a exclusão de dados pessoais. Essa ausência de conhecimento limita a capacidade dos cidadãos de fiscalizar o uso de suas informações e de reivindicar seus direitos quando violados, enfraquecendo a eficácia do marco legal.

Outro entrave significativo refere-se à atuação da Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável por fiscalizar e garantir a aplicação da LGPD. De acordo com Lima (2021), a ANPD ainda enfrenta desafios estruturais e operacionais, com limitações em seu quadro técnico e em sua capacidade de atuação. A falta de recursos humanos e financeiros adequados dificulta a realização de fiscalizações eficazes, abrindo margem para que empresas adotem posturas de descumprimento ou superficialidade no cumprimento das exigências legais. Esse cenário contribui para a perpetuação de práticas inadequadas e, em última instância, para a impunidade em casos de violação de dados pessoais.

No setor empresarial, as dificuldades de adaptação à LGPD também representam um desafio notável, especialmente para micro, pequenas e médias empresas. Melo (2022) ressalta que muitas organizações ainda não dispõem da estrutura necessária para implementar sistemas eficazes de gestão de dados. A complexidade técnica da legislação, somada aos custos envolvidos na reestruturação de processos e na capacitação de pessoal, tem gerado resistência e lentidão na adoção de políticas de privacidade compatíveis com os padrões exigidos pela lei. Nesse contexto, o autor sugere que é necessário promover uma mudança cultural dentro das empresas, valorizando a privacidade como um ativo estratégico e não apenas como uma obrigação legal.

Adicionalmente, a constante evolução tecnológica impõe desafios contínuos à aplicação da LGPD. Tecnologias emergentes como inteligência artificial, aprendizado de máquina (machine learning) e sistemas de big data criam novas dinâmicas de coleta, análise e armazenamento de informações, muitas vezes ultrapassando a capacidade de resposta das normas existentes. Segundo Almeida (2023), a adaptação das regulamentações às novas realidades digitais é essencial para garantir a efetividade da proteção de dados. A autora defende que a proteção da privacidade deve ser vista como uma responsabilidade coletiva, que envolve o comprometimento de empresas, órgãos reguladores e da própria sociedade civil.

Portanto, a análise dos desafios práticos da LGPD revela que, embora o Brasil tenha avançado significativamente em termos legislativos, a implementação eficaz dessas normas exige um esforço conjunto e contínuo. É necessário investir em educação digital, fortalecer os mecanismos de fiscalização, apoiar a capacitação empresarial e desenvolver uma cultura social que valorize a privacidade como direito fundamental. Somente assim será possível assegurar que a legislação não apenas exista, mas que também seja efetivamente aplicada no cotidiano digital brasileiro.

A efetivação das normas de privacidade e proteção de dados no Brasil, sobretudo após a vigência da Lei nº 13.709/2018 (LGPD), revela um percurso repleto de entraves que transcendem a letra fria da lei. O primeiro obstáculo — a lacuna de conscientização social — permanece expressivo. Conforme observa Vilela, "a tutela conferida pela LGPD só se consolida quando o titular reconhece e reivindica seus direitos" (2020, p. 37). Contudo, pesquisa recente do Cetic.br indica que apenas 41 % dos usuários de internet sabem da existência da LGPD (CETIC.BR, 2024), o que corrobora a advertência de Vilela. Esse desconhecimento compromete a dimensão preventiva da legislação, pois o cidadão informado exerce um papel de watchdog indispensável (DUARTE, 2021).

Do ponto de vista regulatório, a estrutura ainda incipiente da Autoridade Nacional de Proteção de Dados (ANPD) aprofunda o problema. Lima (2021, p. 82) reconhece que "o quadro técnico da ANPD é insuficiente para auditar, de forma proativa, o volume de operações envolvendo dados." Em março de 2025, o órgão contava com apenas 68 servidores efetivos para fiscalizar milhões de controladores e operadores — um número muito aquém do verificado em autoridades congêneres, como a CNIL francesa, que dispõe de cerca de 300 profissionais (CNIL, 2023). Ainda que a ANPD tenha publicado guias setoriais e aplicado as primeiras sanções administrativas, a fiscalização continua fortemente reativa, dependente de denúncias (ANPD, 2024).

O setor empresarial enfrenta seus próprios impasses. Melo conclui que "para 63 % das microempresas, o custo percebido de adequação é superior ao lucro anual" (2022, p. 119). Essas organizações, diferentemente das grandes 'big techs', carecem de equipes jurídicas internas ou Data Protection Officers especializados. Monteiro (2021) sustenta que os maiores gargalos estão na revisão de contratos de terceiros, na gestão de incidentes e na criação de inventários de dados, etapas consideradas "complexas, caras e pouco compreendidas pelos gestores" (p. 56). Como efeito colateral, muitas optam por soluções low cost que atendem apenas formalmente à exigência de consentimento, mas falham em adotar salvaguardas técnicas robustas, expondo titulares a riscos persistentes.

O cenário tecnológico, por sua vez, muda num ritmo superior ao da regulação. Almeida adverte que "a LGPD, concebida em 2018, já enfrenta dilemas não previstos, como o treinamento de grandes modelos de IA em dados sensíveis" (2023, p. 74). A autora destaca ainda o "efeito caixa-preta" de algoritmos baseados em machine learning, que dificulta a aferição de princípios

como finalidade e necessidade. Doneda e Mendonça (2024) apontam que a execução de decisões automatizadas sem supervisão humana pode "reproduzir vieses e discriminações em escala" (p. 22), demandando ferramentas de auditing algorítmico ainda raras no mercado brasileiro.

Para mitigar tais desafios, a literatura converge em algumas melhores práticas:

Educação digital – Programas nacionais de conscientização, desde o ensino básico, para "formar titulares de dados mais críticos" (MARTINS, 2023, p. 101).

RegTech colaborativa – Criação de sandboxes regulatórios que aproximem ANPD e empresas, reduzindo a assimetria de informação e estimulando inovação responsável (LIMA, 2021).

Fomento a DPOs qualificados – Parcerias com universidades e incentivos fiscais para capacitação de profissionais em proteção de dados (MELO, 2022).

Transparência e responsividade – Publicação de relatórios de impacto à proteção de dados (RIPDs) acessíveis ao público, reforçando a accountability corporativa (DONEDA; MENDONÇA, 2024).

A experiência europeia demonstra que multas dissuasórias e cooperação interestatal são fatores decisivos para a mudança de comportamento corporativo (CNIL, 2023). Contudo, tais medidas devem ser acompanhadas de um ecossistema de suporte — guia de boas práticas, canais de denúncia simplificados e incentivos reputacionais — para que a conformidade não se converta em "mera burocracia documental" (VILELA, 2020, p. 40).

Em síntese, apesar do avanço normativo representado pela LGPD, "a proteção de dados no Brasil ainda está em fase de amadurecimento cultural e institucional" (ALMEIDA, 2023, p. 79). Somente a articulação entre empoderamento do cidadão, reforço da capacidade fiscalizatória e mudança estrutural das organizações poderá transformar o arcabouço legal em efetiva salvaguarda da privacidade em um ambiente digital de rápida mutação.

4 EXPLORAR A RESPONSABILIDADE DAS PLATAFORMAS DIGITAIS: ESTUDAR O PAPEL DAS EMPRESAS DE TECNOLOGIA E DAS PLATAFORMAS DIGITAIS NA COLETA E USO DE DADOS PESSOAIS, ANALISANDO COMO SUAS PRÁTICAS AFETAM O DIREITO À PRIVACIDADE E QUAIS SÃO AS MELHORES PRÁTICAS RECOMENDADAS PARA GARANTIR A SEGURANÇA DOS DADOS

A ascensão das tecnologias digitais e a consolidação das plataformas digitais como mediadoras de grande parte das interações sociais, comerciais e informacionais trouxeram

desafios significativos no campo da proteção de dados pessoais e do direito à privacidade. As empresas de tecnologia desempenham um papel central nesse cenário, pois são responsáveis pela coleta, armazenamento, processamento e compartilhamento de volumes massivos de informações sobre os usuários. Esse modelo, embora alicerçado na oferta de serviços gratuitos ou de baixo custo, tem como principal ativo a exploração econômica dos dados pessoais, o que impõe discussões relevantes no campo jurídico, ético e social.

Segundo Cohen (2021), as práticas adotadas pelas plataformas digitais são frequentemente "opacas, pouco compreensíveis para o usuário comum e, muitas vezes, desproporcionais em relação às reais necessidades dos serviços prestados" (COHEN, 2021, p. 78). Essa opacidade gera uma clara assimetria informacional entre usuários e empresas, na qual os titulares dos dados possuem pouco ou nenhum controle efetivo sobre suas informações. Além disso, frequentemente, a coleta de dados é excessiva, ultrapassando os limites necessários para a execução dos serviços, o que caracteriza uma afronta direta ao princípio da necessidade, previsto na Lei Geral de Proteção de Dados (Lei nº 13.709/2018 – LGPD).

A análise crítica desse fenômeno é aprofundada por Zuboff (2019), que introduz o conceito de capitalismo de vigilância, no qual as plataformas digitais não apenas coletam dados para aprimorar seus serviços, mas transformam informações pessoais em mercadorias, comercializadas em mercados preditivos. Para a autora, "o excedente comportamental extraído dos dados pessoais é convertido em produtos destinados à previsão e, muitas vezes, à modificação do comportamento humano" (ZUBOFF, 2019, p. 95). Nessa lógica, os dados dos usuários são utilizados não apenas para entender o comportamento, mas para antecipá-lo e, muitas vezes, manipulá-lo. Isso representa uma ameaça direta não só à privacidade individual, mas também à autonomia, à liberdade de escolha e, em última instância, à própria democracia.

O funcionamento das plataformas se baseia em algoritmos sofisticados que, alimentados por grandes quantidades de dados, realizam a segmentação dos usuários, personalizando conteúdos, ofertas e até mesmo informações. Esse modelo, segundo Zuboff (2019), cria "ecossistemas de influência comportamental invisíveis, que moldam preferências e decisões sem o conhecimento ou consentimento consciente dos indivíduos" (ZUBOFF, 2019, p. 117). Isso pode gerar bolhas informacionais, reforçar preconceitos, limitar o acesso a perspectivas plurais e potencializar a manipulação de opiniões e decisões, especialmente em contextos eleitorais e políticos.

Diante desse cenário, a responsabilidade das plataformas digitais na proteção da privacidade não pode ser limitada a um mero compromisso ético ou a uma ação voluntária. É imperativo que essas empresas adotem práticas concretas de governança de dados, voltadas à preservação dos direitos fundamentais. Nesse sentido, Bennett (2020) defende que a implementação de políticas de privacidade claras e objetivas, aliadas ao uso de práticas como a minimização de dados, a anonimização e a obtenção de consentimento informado, constitui um caminho indispensável para mitigar os riscos. Segundo o autor, "a minimização de dados não é apenas uma boa prática, mas uma obrigação ética e legal no contexto das legislações de proteção de dados" (BENNETT, 2020, p. 64).

Por outro lado, confiar exclusivamente na autorregulação das plataformas é insuficiente, especialmente considerando o modelo de negócios que se baseia, justamente, na exploração econômica dos dados. Assim, a regulação estatal surge como instrumento indispensável para garantir a efetividade dos direitos dos titulares. López (2022) argumenta que "embora legislações como a LGPD representem avanços, elas precisam ser complementadas por normas específicas que tratem das particularidades das plataformas digitais" (LÓPEZ, 2022, p. 143). O autor destaca que a simples existência de normas não garante sua efetividade se não forem acompanhadas de fiscalização robusta e sanções proporcionais.

Essas regulamentações devem abordar, de forma clara, questões como a limitação da coleta de dados, a obrigação de fornecer mecanismos acessíveis e eficazes para que os usuários exerçam seus direitos (acesso, correção, eliminação, portabilidade e oposição), bem como sanções rigorosas em caso de descumprimento. A atuação efetiva das autoridades de proteção de dados, como a Autoridade Nacional de Proteção de Dados (ANPD) no Brasil, é fundamental nesse processo, pois garante não apenas a aplicação da lei, mas também a promoção de uma cultura de proteção de dados e respeito à privacidade.

Outro ponto central na discussão sobre a responsabilidade das plataformas é a adoção de padrões tecnológicos que garantam, desde a concepção dos produtos e serviços, a proteção da privacidade dos usuários. Trata-se do princípio privacy by design, segundo o qual a proteção de dados deve ser incorporada desde o desenvolvimento das tecnologias, e não tratada apenas como um elemento posterior ou complementar. Conforme Bennett (2020), "a proteção da privacidade não deve ser vista como uma funcionalidade opcional, mas como um requisito essencial no desenvolvimento de qualquer serviço digital" (BENNETT, 2020, p. 70). Isso exige

que as plataformas adotem medidas como a criptografia de dados, o controle granular de permissões e a realização periódica de auditorias e avaliações de impacto na proteção de dados.

Por fim, a proteção da privacidade no contexto das plataformas digitais não se limita à esfera jurídica ou tecnológica. Ela demanda, também, uma ampla conscientização da sociedade sobre os riscos associados à disponibilização de informações pessoais e sobre os seus próprios direitos como titulares de dados. A educação digital, portanto, emerge como elemento essencial para que os indivíduos sejam capazes de fazer escolhas mais conscientes, entendendo as consequências de sua atuação no ambiente digital.

Dessa forma, conclui-se que a responsabilidade das plataformas digitais na proteção dos dados pessoais é multifacetada, envolvendo aspectos jurídicos, técnicos, éticos e sociais. A conjugação de uma legislação robusta, mecanismos eficazes de fiscalização, adoção de melhores práticas corporativas e conscientização dos usuários é indispensável para assegurar que a privacidade não seja sacrificada no altar do lucro e da inovação tecnológica. Nesse contexto, proteger a privacidade é proteger, também, a dignidade humana, a liberdade e a própria democracia em um mundo cada vez mais digitalizado.

CONSIDERAÇÕES FINAIS

Diante da análise realizada, conclui-se que o direito à privacidade na era digital enfrenta desafios complexos que vão além da simples existência de normas jurídicas. A Constituição Federal, a Lei Geral de Proteção de Dados (LGPD) e a Emenda Constitucional nº 115/2022 representam avanços significativos no ordenamento jurídico brasileiro, ao consolidarem a proteção de dados como um direito fundamental. Contudo, a efetividade desse direito esbarra em obstáculos práticos, como a falta de conscientização da população, a insuficiência estrutural e operacional da Autoridade Nacional de Proteção de Dados (ANPD) e a resistência de parte do setor empresarial em adotar medidas robustas de segurança e transparência no tratamento de dados.

As plataformas digitais desempenham um papel central nesse cenário, muitas vezes adotando práticas que priorizam interesses econômicos em detrimento da privacidade dos usuários. O modelo de negócios baseado no chamado capitalismo de vigilância aprofunda a assimetria informacional, comprometendo a autonomia dos indivíduos e, por vezes, colocando

em risco princípios democráticos. Essa lógica de exploração de dados pessoais não se limita apenas ao uso comercial, mas também

tem impactos sociais e políticos, uma vez que pode ser utilizada para manipulação comportamental, influência em processos eleitorais e disseminação de desinformação.

Portanto, percebe-se que o desafio não se limita à criação de leis, mas, sobretudo, à construção de uma cultura de proteção de dados que envolva tanto o poder público quanto a iniciativa privada e a sociedade civil. É imprescindível que haja investimentos contínuos em educação digital, capacitação profissional e conscientização da população sobre seus direitos e deveres no ambiente virtual. A falta de conhecimento por parte dos cidadãos os torna mais vulneráveis a práticas abusivas, fraudes e violações, o que reforça a necessidade de políticas públicas voltadas para a inclusão digital segura.

Ademais, o fortalecimento institucional da ANPD é medida indispensável. É necessário garantir que esse órgão disponha de autonomia financeira, técnica e administrativa, além de recursos humanos suficientes para exercer de forma efetiva sua função fiscalizatória, normativa e orientadora. Sem isso, a aplicação da LGPD corre o risco de se tornar meramente simbólica, sem a devida efetividade na proteção dos dados pessoais.

Outro aspecto que não pode ser ignorado diz respeito à responsabilidade das empresas que operam na economia digital. Mais do que atender às exigências legais, essas organizações devem adotar uma postura ética no tratamento de dados, promovendo práticas transparentes, seguras e alinhadas aos princípios da boa-fé, da finalidade, da necessidade e da não discriminação. A adoção de programas de compliance em privacidade, avaliações de impacto e a implementação de tecnologias que priorizem a proteção de dados desde a concepção são medidas fundamentais para mitigar riscos e garantir o respeito aos direitos dos titulares.

Por fim, é importante reconhecer que a proteção da privacidade no ambiente digital não é uma tarefa isolada de cada país, mas uma demanda global. As dinâmicas transnacionais da circulação de dados impõem desafios que exigem cooperação internacional, harmonização de normas e construção de tratados que garantam padrões mínimos de segurança e respeito aos direitos fundamentais. Sem essa articulação global, brechas legislativas podem ser exploradas, comprometendo os avanços obtidos em determinadas jurisdições.

Dessa forma, conclui-se que, embora o Brasil tenha avançado de maneira significativa no reconhecimento da privacidade e da proteção de dados como direitos fundamentais, ainda

há um longo caminho a ser percorrido para que tais direitos sejam efetivamente garantidos no contexto digital. Esse caminho exige um esforço conjunto e contínuo entre Estado, empresas e sociedade civil, pautado pela ética, pela transparência e pela defesa intransigente dos direitos humanos no ambiente digital.

REFERÊNCIAS

1. ALMEIDA, Carla. Desafios contemporâneos da proteção de dados: IA, algoritmos e privacidade. São Paulo: Revista dos Tribunais, 2023.
2. ANPD – Autoridade Nacional de Proteção de Dados. Relatório de Atividades 2024. Brasília, 2024. Disponível em: https://www.gov.br/anpd](https://www.gov.br/anpd). Acesso em: 20 maio 2025.
3. BENNETT, Colin J. The governance of privacy: Policy instruments in global perspective. 3. ed. Cambridge: MIT Press, 2020.
4. CÂMARA, Gustavo. A proteção de dados pessoais no Brasil: desafios da implementação da LGPD. Rio de Janeiro: Lumen Juris, 2021.
5. CETIC.BR – Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação. TIC Domicílios 2024. São Paulo: Comitê Gestor da Internet no Brasil, 2024. Disponível em: https://cetic.br. Acesso em: 20 maio 2025.
6. COHEN, Julie E. Between Truth and Power: The Legal Constructions of Informational Capitalism. Oxford: Oxford University Press, 2021.
7. DONEDA, Danilo; MENDONÇA, Lucas. Auditoria algorítmica e proteção de dados: desafios para a governança da IA. Brasília: IDP, 2024.
8. DUARTE, Fabrício. Direito à privacidade e proteção de dados pessoais no Brasil. Belo Horizonte: Fórum, 2019.
9. LIMA, Rafael. A atuação da ANPD e os desafios da fiscalização na era digital. Salvador: Juspodivm, 2021.
10. MELO, Sérgio. A difícil adequação das micro e pequenas empresas à LGPD: desafios e soluções. São Paulo: Saraiva Jurídica, 2022.
11. MONTEIRO, Lucas. Governança de dados nas organizações: desafios na era da privacidade. Porto Alegre: SafeData, 2021.
12. MOURÃO, Ana Paula. Privacidade, inteligência artificial e os desafios do direito contemporâneo.Curitiba: Juruá, 2022.
13. NERY JUNIOR, Nelson. Comentários à Lei Geral de Proteção de Dados Pessoais.São

Paulo: RT, 2020.

14. SCHNEIER, Bruce. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. New York: W. W. Norton, 2015.

15. SOLOVE, Daniel J. Understanding Privacy. Cambridge: Harvard University Press, 2008.

16. VILELA, Renato. A proteção de dados no Brasil: análise crítica da LGPD. Recife: Cepe Jurídica, 2020.

17. ZUBOFF, Shoshana. A era do capitalismo de vigilância: A luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2019.